USER GUIDE

T3 PowerBroadband

Motorola, Inc.

570510-001-00 rev A

Motorola, Inc.
5200 Franklin drive, Suite 100
Pleasanton, CA 94588
1 (925) 201-4500 main
1 (925) 201-4509 fax
1 (800) 998-4888
www.systems.com
Published in the United States of America
August, 2007
T3 PowerBroadband User Guide
Text part number: 570510-001-00 rev A

Model Number: 45225
45101

Radio Frequency Interference Requirements- FCC
Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Radio Frequency Interference Requirements- Canada
This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Marking and European Economic Area (EEA)
WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Statement of Compliance
Motorola/Symbol hereby declares that this device is in compliance with all the applicable Directives, 2004/108/EC and 2006/95/EC. A Declaration of Conformity may be obtained from http://www2.symbol.com/doc/.

Model Number: 45010

Wireless Device Country Approvals
For 2.4GHz or 5GHz Products: Europe includes, Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Operation of the device without regulatory approval is illegal.

Frequency of Operation – FCC and IC
2.4 GHz Only
The available channels for 802.11 b/g operation in the US are Channels 1 to 11. The range of channels is limited by firmware.

RF Exposure Guidelines
Safety Information

Reducing RF Exposure – Use Properly

Only operate the device in accordance with the instructions supplied.

International
The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices. For information on “International” human exposure to eletromagnic fields refer to the Motorola/Symbol Declaration of Conformity (DoC) at http://www2.symbol.com/doc/.

EU
Remote and Standalone Antenna Configurations

To comply with EU RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop of similar configurations must operate with a minimum separation distance of 20 cm from all persons.

FCC
Remote and Standalone Antenna Configurations

To comply with FCC RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop of similar configurations must operate with a minimum separation distance of 20 cm from all persons.

To satisfy FCC RF exposure requirements, a mobile transmitting device must operate with a minimum separation distance of 20 cm or more from a person's body.

Radio Frequency Interference Requirements- FCC
Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Radio Transmitters (Part 15)
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radio Frequency Interference Requirements- Canada
This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Radio Transmitters
This device complies with RSS 210 of Industry & Science Canada. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Label Marking: The Term "IC:" before the radio certification only signifies that Industry Canada technical specifications were met.

Marking and European Economic Area (EEA)
WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

The use of 2.4GHz WLAN's, for use through the EEA, have the following restrictions:

- Maximum radiated transmit power of 100 mW EIRP in the frequency range 2.400 -2.4835 GHz.
- France, outside usage is restricted to 2.4 – 2.454 GHz.
- Italy requires a user license for outside usage.

Statement of Compliance

Motorola/Symbol hereby, declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. A Declaration of Conformity may be obtained from http://www2.symbol.com/doc/.

IMPORTANT SAFETY INSTRUCTIONS

T2-2500 and T3 Switch
CAUTION: For installation only in a Restricted Access Location by trained service personnel.
CAUTION: Equipment must be connected to an earthed mains socket-outlet.
CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
CAUTION: The power supply cord plug serves as the main disconnect for the product. The socket-outlet shall be installed near the product and be readily accessible.
CAUTION: Voltages present which are above TNV-3 (POTS) limits. A cover must be installed over the punch down blocks with a HV (High Voltage) warning label (supplied).

The maximum operating ambient temperature is 50 degrees Celcius.

When installing the Switch in an equipment rack, consider the following potential hazards:

Elevated Operating Ambient Temperature – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).
Reduced Air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained.
Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

m2 WallPlate
CAUTION: Use only power supplies listed in the user manual
When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.

SAVE THESE INSTRUCTIONS

Waste Electrical and Electronic Equipment (WEEE)

English: For EU Customers: All products at the end of their life must be returned to Motorola for recycling. For information on how to return product, please go to: www.motorola.com/recycling/weee.

Bulgarish: За клиенти от ЕС: След края на полезния им живот всички продукти трябва да се връщат на Motorola за рециклиране. За информация относно връщането на продукти, моля отидете на адрес: www.motorola.com/recycling/weee.

Dansk: Til kunder i EU: Alle produkter skal returneres til Motorola til recirkulering, når de er udtjent. Læs oplysningerne om returnering af produkter på: www.motorola.com/recycling/weee.

Deutsch: Für Kunden innerhalb der EU: Alle Produkte müssen am Ende ihrer Lebensdauer zum Recycling an Motorola zurückgesandt werden. Informationen zur Rücksendung von Produkten finden Sie unter: www.motorola.com/recycling/weee.

Eesti: EL klientidele: kõik tooted tuleb nende eluea lõppedes tagastada taaskasutamise eesmärgil Motorola'ile. Lisainformatsiooni saamiseks toote tagastamise kohta külastage palun aadressi: www.motorola.com/recycling/weee.

Español: Para clientes en la Unión Europea: todos los productos deberán entregarse a Motorola al final de su ciclo de vida para que sean reciclados. Si desea más información sobre cómo devolver un producto, visite: www.motorola.com/recycling/weee.

Français : Clients de l'Union Européenne : Tous les produits en fin de cycle de vie doivent être retournés à Motorola pour recyclage. Pour de plus amples informations sur le retour de produits, consultez: www.motorola.com/recycling/weee.

Italiano: per i clienti dell'UE: tutti i prodotti che sono giunti al termine del rispettivo ciclo di vita devono essere restituiti a Motorola al fine di consentirne il riciclaggio. Per informazioni sulle modalità di restituzione, visitare il seguente sito Web: www.motorola.com/recycling/weee.

Magyar: Az EU-ban vásárlóknak: Minden tönkrement terméket a Motorola vállalathoz kell eljuttatni újrahasznosítás céljából. A termék visszajuttatásának módjával www.motorola.com/recycling/weee.

Nederlands: Voor klanten in de EU: alle producten dienen aan het einde van hun levensduur naar Motorola te worden teruggezonden voor recycling. Raadpleeg www.motorola.com/recycling/weee voor meer informatie over het terugzenden van producten. www.motorola.com/recycling/weee.

Português: Para clientes da UE: todos os produtos no fim de vida devem ser devolvidos à Motorola para reciclagem. Para obter informações sobre como devolver o produto, visite: www.motorola.com/recycling/weee.

Românesc: Pentru clienții din UE: Toate produsele, la sfârşitul duratei lor de funcționare, trebuie returnate la Motorola pentru reciclare. Pentru informații despre returnarea produsului, accesați: www.motorola.com/recycling/weee.

Slovenski: Za kupce v EU: vsi izdelki se morajo po poteku življenjske dobe vrniti podjetju Motorola za reciklažo. Za informacije o vraèilu izdelka obišèite: www.motorola.com/recycling/weee.

Suomi: Asiakkaat Euroopan unionin alueella: Kaikki tuotteet on palautettava kierrätettäväksi Motorola-yhtiöön, kun tuotetta ei enää käytetä. Lisätietoja tuotteen palauttamisesta on osoitteessa: www.motorola.com/recycling/weee.

Svenska: För kunder inom EU: Alla produkter som uppnått sin livslängd måste returneras till Motorola för återvinning. information om hur du returnerar produkten finns på www.motorola.com/recycling/weee.

Commands and Syntax

The Motorola T3 PowerBroadband system can be managed via a Command Line Interface, webUI, and SNMP. Commands that apply to remote WallPlates, such as Ethernet port configurations and wireless interface, are all entered on the T3 Switch.

Command Hierarchy

The Command Line Interface (CLI) implements a hierarchical command structure. Commands are organized as a high-level command keyword related to a particular function of the device with sub-commands related to sub-functions.

You may move down in the command hierarchy by entering root keywords and sub-keywords followed by the enter key. Your current level in the command hierarchy is referred to as the "command context." The top-level context is referred to as the "root command context." You may move up to the previous command context by using the exit command. The command prompt is the system name, followed by the current command context.

For example, the root command prompt with the default configuration is:

```
system>
```

Full commands may be entered at the root command context. For example:

```
system> interface dsl enable port1
```

You may also move down levels in the command hierarchy, which allows you to execute commands with less repetitive typing.

For example:

```
system> interface
system:interface> dsl
system:interface.dsl> enable port1
system:interface.dsl> enable port3
system:interface.dsl> enable port3
system:interface.dsl> exit
system:interface> exit
system>
```

Administrative Commands

Most commands discussed in this guide are administrative commands, which change the configuration of the system or affect the operation of the system. These commands can only be executed from the **admin** account. Configuration changes take affect immediately and are recorded in non-volatile memory (NVRAM) in the default mode. Alternatively, you may choose not to record changes in NVRAM. In this case, changes will need to be committed before rebooting the system; otherwise the configuration will revert to the last saved configuration. If automatic commit is enabled, or the configuration is manually committed, the running configuration will automatically be restored if the system power cycles or is rebooted.

Show Commands

The **show** commands are used to view configurations, status and/or statistics. These commands can be issued from either the **user** or **admin** account.

Global Commands

Commands that are available from any command context are called *global* commands. For example, the **help** command can be used whether you are at the root command context or down a few levels in the command hierarchy. Global commands can also be used from either the **user** or **admin** account.

> **Note:** The default prompt is "system>". If you set the system name using the "**system name**" command, the prompt changes to the new system name.

Command	Description
clear	Clears the screen
exit	Use this command to switch to the previous context. Note that using the **exit** command at the root command context performs the same function as logout.
help	Displays the help files
history	Shows the history of the commands used in the current session.
logout	Can be used with either the login (admin, user, RADIUS network authenticated) and at any command level to terminate the current session
tree	Shows the structure of the command tree

Command Completion

The CLI allows you to shorten commands as long as the characters are not ambiguous. While typing a command, press the tab key to have the system complete the current command word or type (**?)** to have the system display a list of available options. The options displayed vary according to the context:

• If you type a **?** at a prompt, the system displays a list of all available commands.
• If you type an unambiguous command word, pressing **?** displays all available subcommands or arguments. For example, **show ?** (note the space before the question mark) displays a list of all show subcommands.

Style Conventions

The style conventions used in this manual distinguish various elements of the commands and facilitate the proper interpretation of command syntax, parameters, and their use.

Keyword	Show the actual text you must enter. A keyword is found within carrots <>, followed by an input parameter. You must type the keyword, followed by the parameter.
<ip-address>	Indicates the text is a variable where you must supply the actual value
[ ]	Square brackets delimit optional keywords or arguments. One or more of these optional parameters can be entered on the same line. For example, the "interface wireless config" command has 12 optional parameters of which you can choose only the parameters you want to configure.
-	Hyphens are used to indicate remote ports on a connected WallPlate. Port numbers following the hyphen are remote Ethernet ports or remote WLANs.

For example:

interface wireless enable <radio<1-25>(interface-id)>

where;
"radio" is a keyword and must be typed
<1-25> is a port range parameter for the wireless radio connected to the DSL line
(interface-id) is a description and is not typed

Proper command form:

interface wireless enable radio5

wifi wlan enable <wlan<1-25>-<1-16>(interface-id)>

where;
“wlan” is a keyword and must be typed
<1-25> is the port range for the radio connected to the DSL line
<1-16> is the port range of the WLAN on the radio
(interface-id) is a description and is not typed

Proper command form:

wifi wlan enable wlan25-1

Note that range commands can also be used. In the following example, WLANs 1, 2, 3 are enabled on all radios.

wifi wlan enable wlan(1-25)-(1-3)

This document refers to actual command syntax as little as possible. For a complete command syntax document, please refer to the *Command Reference* guide for a complete list of all available commands, the proper syntax, and usage examples. In no way does this User Guide attempt to replace or obsolete the *Command Reference*.

Interface Range

Multiple interfaces can be specified for a single command using port ranges. Use hyphens (-) and commas (,) to delineate ports. Port numbers must be contained in parenthesis. Hyphens and commas can be combined in the same expression to specify multiple, non-sequential interfaces. For example;

To enable all 25 DSL ports, type: *interface dsl enable port(1-25)*

To enable only selected DSL ports, type: *interface dsl enable port(1,3,5,20-25)*

Hyphens and commas can also be used to enable remote Ethernet ports along with DSL ports. For example;

To enable Eth1 and Eth2 on every WallPlate, type: *interface remote enable port(1-25)-(1,2)*

VLAN commands can also be completed using interface ranges.

To add VLAN 100 to Eth1 on every WallPlate, type: *vlan membership add 100 interface port(1-25)-1*

System Description

The T3 PowerBroadband system is designed primarily for hospitality, but useful in any high density MDU (multiple dwelling unit) such as long term healthcare or centrally wired apartments. The system is comprised of two primary components; a 25-port Switch and a CPE device (the WallPlate). Advanced networking features such as 802.1Q VLANs and QoS can be managed throughout the system, from the 25-port switch to each port on the WallPlate.

Adaptive Line Power

T3 PowerBroadband delivers operating power to the remote WallPlates.

MC-802 Wireless WallPlate	Line powered up to 300m (1000ft)
M2 Ethernet WallPlate	Line powered up to 600m (2000ft)

T3 PowerBroadband Switch

The T3 switch is installed in a centrally located phone room; where all the telephone wires converge. The T3 switch has 25 ports for downstream WallPlates, and 2 x GigE uplink ports.

T3 PowerBroadband Switch:

Physical

- 17.50"(43.8mm) x 14.25" (36mm) x 1.75" (44mm). 11.5lbs (5.2Kg)
- Operating Temperature: 0 - 50 degrees Celsius, 5% to 90% NC
- Operating Power: 300W maximum under full load, 200W typical

Interfaces

- Uplink ports
  - Two 10/100/1000Mb autosensing, full duplex Ethernet ports via RJ45
- Downlink ports
  - 25 VDSL UTP ports via RJ21 telco connector

Layer-2 Networking Features

- 802.1Q VLAN trunk ports
- 802.1Q PVID per port
- Port-based Isolation VLANs
- QoS, 4 queues per port, classification by IP-TOS or L2-COS bit
- IGMP, Layer 2+ routing, proxy, FastLeave
- 1024 entry MAC forwarding table

Management

- Telnet, Console, webUI, Syslog, SNMPv2c
- RADIUS authentication, Admin and User level login
- Security: L2 VLAN, IP ACL

M2 Ethernet WallPlate

The m2 Ethernet WallPlate has two 10/100Mb Ethernet ports, and a pass-through RJ11 phone connector. It is installed at the end-point where Ethernet service is desired. It operates over a standard 2-wire telephone line.

M2 Ethernet WallPlate:

Physical
- 5"(mm) x 3.5" (mm) x 1.25" (32mm)
- Operating Temperature: 0 - 40 degrees Celsius, 5% to 90% NC
- Operating Power: approximately 2W, line powered by the T3 Switch

Interfaces
- Uplink ports
  - One VDSL single wire pair port via RJ11 jack
- Downlink ports
  - Two 10/100Mb autosensing, full duplex Ethernet port via RJ45 jack
  - One pass-through filtered phone port via RJ11 jack

Layer-2 Networking Features
- 802.1Q VLAN trunk ports
- 802.1Q PVID per port
- QoS, 2 queues per port, port based classification

Management
- Embedded Layer-1 channel for device management from T3 Switch

MC-802 Wireless WallPlate

The MC-802 Wireless WallPlate has two 10/100Mb Ethernet ports, a pass-through RJ11 phone connector, and a managed 802.11b/g radio. It is installed at the end-point where Ethernet and/or Wireless service is desired. It operates over a standard 2-wire telephone line.

Features of the MC-802 802.11b/g radio:

Physical
- 6.625"(168mm) x 3.75" (95.25mm) x 1.75" (44.45). lbs (Kg)
- Operating Temperature: 0 - 40 degrees Celsius, 5% to 90% NC
- Operating Power: approximately 6W, line powered by the T3 Switch

Interfaces
- Uplink ports
  - One VDSL single wire pair port via RJ11 jack
- Downlink ports
  - Two 10/100Mb autosensing, full duplex Ethernet port via RJ45 jack
  - One 802.11b/g radio
  - One pass-through filtered phone port via RJ11 jack

Layer-2 Networking Features
- 802.1Q VLAN trunk ports
- 802.1Q PVID per port
- QoS, 4 queues per port

Management
- Embedded Layer-1 channel for device management from T3 Switch
- Layer-3 IP addresses from private pool or public pool
- All management centralized on T3 Switch

Radio

- 802.11b/g
  - Beacon frame control
  - Probe request response
  - Broadcast on/off per SDID
  - Listen mode client support
  - DSS/OFDM modulation via 2.4Ghz transmitter
  - Regulatory Domain: FCC Part 15c 15.247 and ETS 300 328
- Transmit power: 20dBm transmitter
  - Customer configurable: 1 – 14, max. In 1dBm increments
  - Max transmit power of 20dBm depends on regulatory country
- Two integrated omni-directional antennas
  - 3.2dBi
  - Antenna receive diversity
- Security Protocols – (per SSID)
  - Wireless Client Isolation
  - WEP/WPA/WPA2 - Enterprise
  - 802.1x/EAP
  - EAP types: TLS, PEAPv0, TTLS
  - AES, TKIP encryption
- QoS
  - Wireless Multimedia (WMM) priority
  - WMM power save
  - Spectralink ready
- Virtual AP mode
  - Concurrent BSS (16)
  - Per-BSS SSID
  - Per-BSS client isolation
  - Per-BSS 802.1Q VLANs
  - Per-BSS authentication/encryption
  - Per-BSS bitrate
- Two runtime images in flash, realtime firmware upgrade
- Client state, status and statistics
  - MAC address of client
  - Client link rate
  - Client link strength (dBm)
  - Packets tx/rx
  - Authentication status
  - SSID
  - MAC address
- WLAN state information
  - Signal strength and MAC of other APs
  - Tx signal strength
  - Packet Tx/Rx statistics

Hardware

Model Numbers and Description

The T3 PowerBroadband Switch is compatible with both the Wireless and Ethernet WallPlates. Both can be mixed together on the same T3 PowerBroadband Switch.

Model Number	Part Number	Description
45225	558975-001-00	T3 PowerBroadband Switch. 2 x 10/100/1000Mb uplink Ethernet ports and 25 x high speed DSL ports for connection to UTP wiring. Provides broadband data and Adaptive Line Power for remote wireless WallPlates. Supports 45010 and 45101. RoHS compliant.
45010	557925-001-00	MC-802 Wireless WallPlate. 1 x 802.11 b/g radio, 2 x Fast Ethernet, 1 x high speed DSL port, 1 x analog POTS RJ11 port. Designed for installation over existing RJ11 wall jack. RoHS compliant.
45101	549478-001-00	2 port m2a WallPlate. 2 x Fast Ethernet ports, 1 x high speed DSL port, 1 x analog POTs RJ11 port. Two powering options; Adaptive Line Power from the 45125 switch, or local power adapter. Designed for installation over existing RJ11 wall jack. RoHS compliant.

Model Numbers and Description for related Products

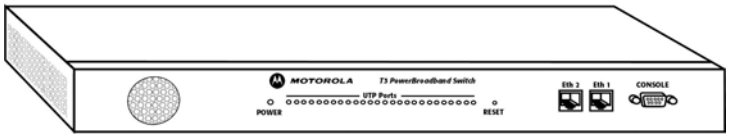
Filters are required for proper in-room installation. Installation may also use one or more of the following additional products.

Model Number	Part Number	Description
65601	552689-001-00	In-line RJ11 filter, T3. RoHS compliant
65602	552309-001-00	In-line unterminated filter, T3. RoHS compliant
65003	552305-001-00	12VDC regulated power supply, US. RoHS compliant. Power supplies used during installation for diagnostics.
65103	552306-001-00	12VDC regulated power supply, Euro. ROHS compliant. Power supplies used during installation for diagnostics.
61299	552304-001-00	RJ11 telephone cable, 2m. RoHS compliant

T3 PowerBroadband Switch

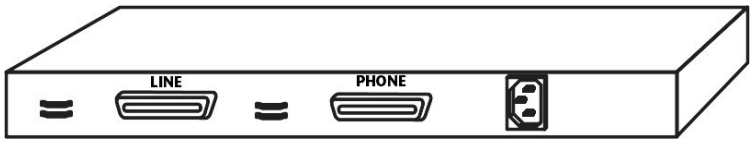
Front View

ETHERNET PORTS: 2 x 10/100/1000 auto-sensing
CONSOLE PORT: DB9 serial

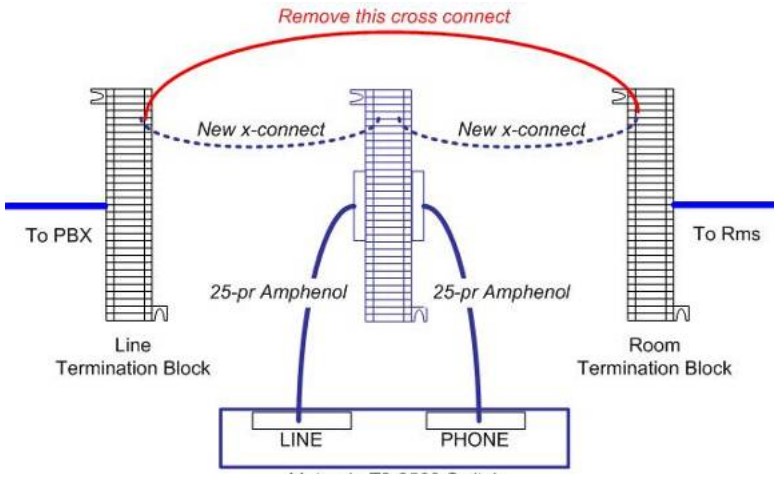


Rear View

LINE RJ21: Connect to PBX side of termination block
PHONE RJ21: Connect to HOUSE side of termination block
AC POWER: 100-240VAC IEC320 socket



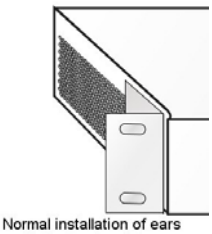
Cross-Connect Connections

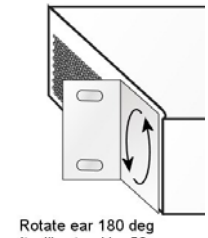


T3 PowerBroadband Switch

Mounting Options

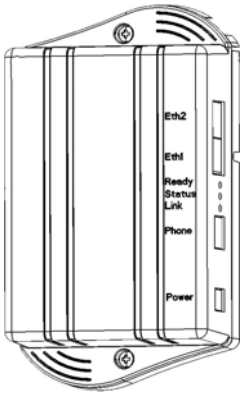
T3 ships with mounting ears designed for a standard EIA-19 equipment rack. The ears can be rotated 180 degrees.





MC-802 Wireless WallPlate

Designed to be installed over existing RJ11 wall jack. Ships with Adapter plate for standard 70mm x 114mm RJ11 wall jack.



Eth1 – 10/100 auto-sensing Ethernet

Eth2 – 10/100 auto-sensing Ethernet

RJ11 filtered phone port

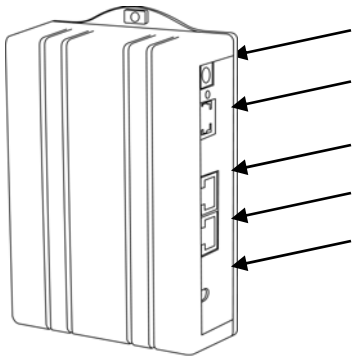
DC power connector (used during installation, not under normal operation)

LED Status Lights

READY	ON solid when the CPU is initialized
STATUS	OFF when no radio config is loaded ON solid when a config is loaded, but the radio is disabled or not transmitting BLINKING when the radio is transmitting
LINK	Flash slow when DSL is enabled but not linking Flash fast when DSL is enabled and training ON solid when DSL is linked

m2 – 2 port Ethernet WallPlate

Designed to be installed over existing RJ11 wall jack. Bracket has a large opening to route the RJ11 cable from the existing jack. See Installation Chapter for a breakout view of the cover and bracket.



DC power connector (used during installation, not under normal operation)

RJ11 filtered phone port

Eth1 – 10/100 auto-sensing Ethernet

Eth2 – 10/100 auto-sensing Ethernet

RJ11 line-in port (not shown, accessible when bracket is removed)

System Administration

This User Guide covers the commands relevant to the T3 PowerBroadband Switch. For a complete set of commands and information, consult the T3 PowerBroadband Command Reference.

Management Access

T3 can be managed via serial console, telnet, HTTP webUI, or SNMP. Eth1 is enabled by default. Telnet and HTTP are accessible at the default IP address.

Access Methods

Default IP address	192.168.1.3
Serial console	Terminal settings: 9600-8-N-1 no flow control
Telnet	Uses TCP port 23
HTTP	Browser support: IE6 or greater, Mozilla based browser Management URL: http://<IP address> IP Port: 80

Default login and password

Default user name for administrative access: admin
Default password: <blank>

Default user name for monitoring only: user
Default password: <blank>

CLI Configuration Script files

T3 file system stores and load configuration script files. These files are text editable. Use the following commands to complete these management tasks:

1. Create a starting configuration file from an existing T3 switch
2. Copy the file to an external server
3. Edit the file on a PC
4. Load the file into another T3 switch
5. Execute the file as a set of configuration commands

The command syntax to use the file system is:

file copy <string(source)> to <string(destination)>

a. Source can be a local file, a remote FTP or TFTP file, or a pre-defined keyword. Keywords allow you to capture the startup and running configuration to a file. Supported keywords are “startup” and “running”.

b. Destination can be a local file or a remote FTP or TFTP file. Note that the combination of the Source keywords and the remote Destination allows you to copy the running config directly to a remote server. For example; file copy running to tftp://192.168.1.1/my-t3-config.txt

c. At least one (source or destination) must be the local file system. If the source and destination are remote servers, the command will fail.

file delete <string(file)>

d. Delete a file from the file system

file dir

e. List the files in the system and display the remaining storage

file exec <string(file)>

f. Executes a file as a set of configuration commands. Note that "file" is a local file in the file system. The file must have previously been copied to the filesystem from the external server using the ***file copy*** command.

Configuration Files using the webUI

From the webUI, the administrator can save and load configuration files. Note that these configuration files are non-editable binary format for configuration security. If editable configuration is desired, use the CLI script files. Configuration files from the webUI can be used to create secure template configurations.

Note: The Configuration File contains every configuration possible including the "Admin" account password. When combined with RADIUS network authentication, the non-editable Configuration Files provide a secure method to pre-configure systems in a staging area and apply the secure "admin" password without revealing the password. Contact a Motorola support person for assistance with a setting up secure, staged configurations.

To save or load a Configuration file from the webUI, access the **System – Configuration** screen from the webUI.

Follow these steps to create a template configuration file:

1. Configure a complete system configuration
2. Set the system name to "template configuration" or similar name
3. Save the configuration file using the webUI System-Configuration screen

Follow these steps to apply the template to a new system:

1. Boot a new system
2. Using the serial console login, set the IP address (or use the default IP address)
3. Reboot the system to apply the IP address
4. Login via the webUI
5. Load the template configuration file using the System-Configuration screen
6. Change the system name to the correct name
7. Change the IP address to the correct IP address
8. Power off or reboot the system. The next time the system is booted, it will have the complete configuration with the correct IP address and system name.

HTTP Menus

Monitor Menu	Quick access to all Ethernet, DSL and Wireless interface status and statistics Color coded Port Monitor: Green - Ethernet Port or DSL Port is operating normally and within tolerance Gray - Ethernet Port is enabled, but disconnected. Yellow - Indicates an alert condition. Red – Indicates a warning or alert condition. When applied to the Line Status, Red indicates the line is enabled, but the WallPlate is disconnected. Black – Port is disabled
System Menu	All configuration items related to setting up the system and management access. For example; IP address, SNMP, image upgrade
Interface Menu	Configure all Ethernet, DSL and Wireless interfaces. Note: the wireless commands under the Interface menu are global commands that apply to all WLANs on a single radio.
Wifi Menu	Configure WLANs. Create up to 20 profiles. Each profile contains unique parameters including SSID, DTIM, Broadcast SSID, Isolation, Timeout, and Security
Advanced Menu	Advanced configurations including 802.1Q VLANs, IGMP, QoS

Upgrading the Firmware

T3 Firmware

T3 Switch stores one active and one alternate boot image.

To view the current image, or to monitor the progress of an upgrade, use:

show system image

The system image can be upgraded using FTP or TFTP. Commands used are:

Using FTP: *system image load ftp://username:password@ipaddress/path/t3-app.img*
Using TFTP: *system image load tftp://ipaddress/path/t3-app.img*

Instructions to obtain and upgrade the system image are found in the release notes of each software image.

Ethernet WallPlate Firmware

The Ethernet WallPlate software image is embedded in the T3 system image. As of the T3 3.0.0 firmware release, no upgrade is required on the Ethernet WallPlates. Check the most current firmware Release Notes to see if an image upgrade will be done on the WallPlate.

At bootup, the image version is checked. If the WallPlate image requires a reload, the time to upload all 25 WallPlates is approximately 20 minutes. Interruption during the upgrade time will not damage the WallPlate. Note, however, that the Ethernet WallPlate will be unable to carry network traffic during image upgrade.

Wireless WallPlate Firmware

The Wireless WallPlate software image is stored in the file system of the T3 Switch and loaded onto the WallPlates from that location. Each Wireless WallPlate stores one active and one alternate image. The image can be upgraded in runtime, user traffic will not be affected. The total time to complete a runtime upgrade of any single WallPlate is approximately 20 minutes. If upgrading multiple WallPlates, the system will automatically stagger the start-time of each unit. Monitor the upgrade process using this command:

show remote image

The status will display a percentage of completion, and show what action is currently being done. Do not reboot the WallPlate until it is 100% complete. Since the WallPlate supports two images, an unintentional interruption will not damage the unit.

Upgrading the software on the Wireless WallPlate requires three steps:

Step 1: FTP or TFTP the Wireless WallPlate image to the file system of the T3 Switch

file copy tftp://<IP of TFTP server>/path/mc800-app.img to mc-800-app.img

NOTE: do not change the name of the file.

Step 2: Load the new image into the alternate image bank on the Wireless WallPlate

remote image load port<x> tftp://<Private IP address of T3>/mc800-app.img

NOTE: for information on IP Addressing refer to pages 24-26, “Managing the Wireless WallPlate”

Step 3: Reboot the Wireless WallPlate to activate the new software

remote image boot port<x> alternate
remote reboot port<x>

Line Quality

T3 includes Forward Error Correction in the VDSL frames. Bit errors that are not corrected are counted and reported as a Line Quality measurement. Bit errors are averaged over 1 second of time. An SNMP trap will be sent to the SNMP trap recipient when the threshold is crossed. The line quality status will change in the webUI and the Command Line Interface. There are two thresholds that will be set:

Maximum threshold – the line quality status will change to Fair when the errors increase beyond the maximum threshold
Minimum threshold – the line quality status will change to Good when the errors decrease below the minimum threshold

To set the line quality threshold, use the following command:

interface dsl thresholds min-threshold <0.5 to 50> max-threshold <0.5 to 50>

Line quality threshold can also be set from the webUI using the **Interface DSL** menu

By default, the thresholds are set to:

min-threshold 1.7 bit errors/second
max-threshold 2 bit errors/second

View System Configuration and Status

Configuration and Status can be viewed using the Show commands. To view the available show items, use the following command from the CLI:

show ?

Ex: View Current and alternate software versions on the system and the WallPlates:

show system image
show system inventory
show remote image
show remote inventory

T3 OS displays the configuration from the CLI in three useful modes. All configuration displays can be accessed from the "show system config" command syntax.

Summary	Use the command: *show system config summary* This command displays the configuration in an organized summary of each configured feature. Use this output to quickly view the active configuration.
Startup	Use the command: *show system config startup* Displays only the commands entered by the administrator that result in a configuration change AND have been saved to memory. Use this command to capture an active configuration and create a template for configuring other XLT switches.
Running	Use the command: *show system config running* Displays only the commands entered by the administrator that result in a configuration change. The changes may or may not have been saved to memory. Use this command to capture an active configuration and create a template for configuring other switches. **Note:** When the commit mode is set to manual, the Running config will be different from the Startup config until the changes are committed.

Commit mode

T3 OS supports automatic and manual commit modes. When in automatic mode, every command will be executed immediately and saved to memory. The commands will be active if the system is rebooted or power cycled.

In manual mode, commands are executed immediately, but are not saved to memory. The commands will be lost when rebooted if they are not committed.

To change the mode:

system config mode <*auto*|*manual*(mode)>

To commit manual commands to memory:

system config commit

Reset to Default Configuration

From the CLI, enter the following command:

system config default

Note: This command is only available from a local serial login session to prevent accidental default from a network login.

Other Configuration Help

The *T3 Command Reference* is the master text for all T3 or T3 PowerBroadband configurations. It contains an alphabetical listing of all CLI commands, syntax and example configuration.

The web UI features a context-sensitive help system.

Managing the Wireless WallPlates

The Wireless WallPlate is managed through two interfaces; one interface is via an embedded management channel within the VDSL frames. The other interface is through a layer 3 IP address.

WallPlate Inventory and Firmware Image

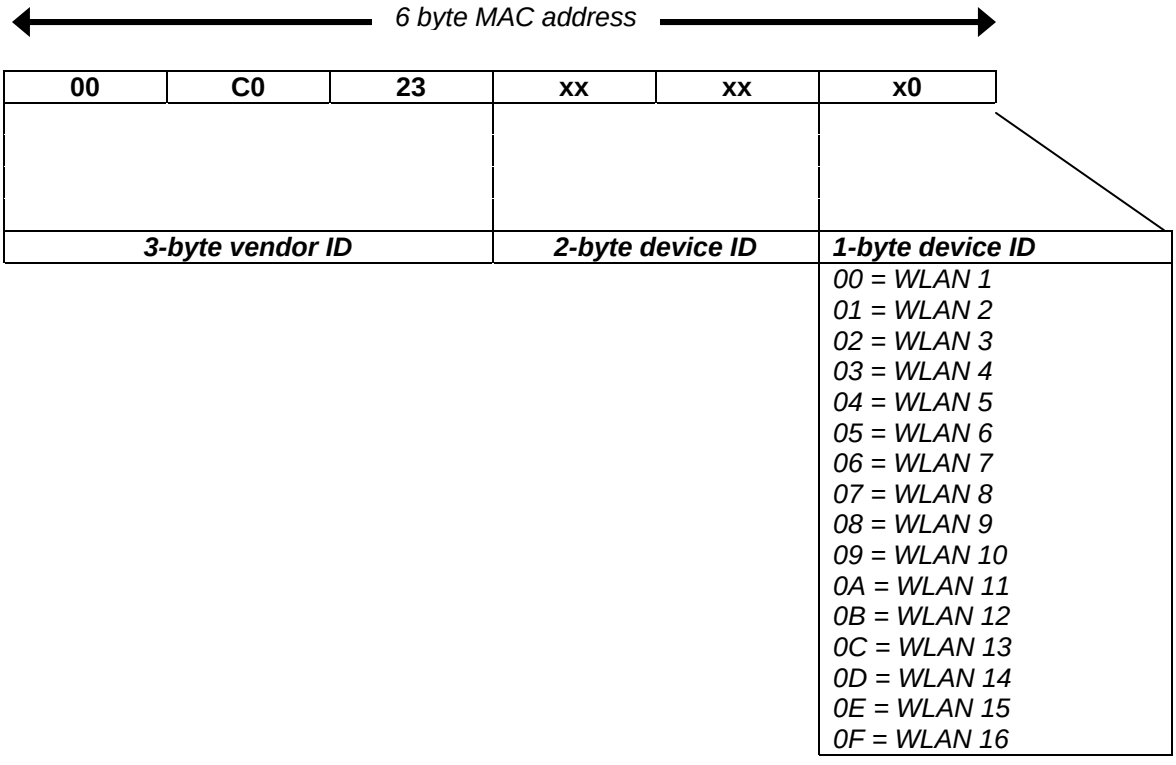
Show remote inventory

"show remote inventory" command uses the embedded channel to read hardware rev and basic information, including serial number and BSS MAC range. Additionally, this out-of-band channel is used to detect the device and initiate communications. This interface can operate if IP addressing is invalid or the system is unable to communicate at Layer 3. This command will read hardware information for the Wireless WallPlate or the m2 Ethernet WallPlate.

Each Wireless WallPlate has 16 MACs, assigned to 16 WLANs. To read the MAC addresses assigned to the WLANs, use;

show remote inventory port<x>

Note that only one MAC address is shown for the BSS. This is the starting MAC, assigned to WLAN 1 on that radio. The remaining 15 WLANs will increment from the last octet, 00.



Show remote image

"show remote image" command uses the layer 3 interface to communicate. Use this command to ensure the T3 has full access to the Wireless WallPlate. Note this command will not read information from an m2 Ethernet WallPlate. If this command stalls, then the T3 cannot communicate. This is most likely an IP addressing mistake.

IP Addresses

Private IP address

The T3 system requires an IP address for network management. This T3 management address is assigned using the following command:

ip config ip-address <your IP> mask <your mask> gateway <your gateway>

The Wireless WallPlates also require an IP address for management by the T3 system. The IP address pool assigned to the Wireless WallPlates can be in the same subnet as the network management IP address, or it can be a private IP address space that is not used outside the T3 system.

The default configuration is to use a private IP address space to manage the Wireless WallPlates.

Note these important operational parameters when using the private IP space to manage Wireless WallPlates:

1. All T3 systems on the same property (same layer 2 network) can use the same private IP space to communicate with their own Wireless WallPlates. There will not be an IP conflict on the network.
2. The Wireless WallPlates will not send ARPs to the upstream Ethernet network.
3. The Wireless WallPlates will not send DHCP requests to the upstream Ethernet network.
4. The default private IP address space is 192.168.10.226 through 192.168.10.250. All WallPlates will be assigned an IP address starting with 192.168.10.226.
5. The default private IP internal address is 192.168.10.1. Use this address when loading new firmware to the Wireless WallPlate from the internal file system on the T3 Switch.

To enable the private IP addressing, type:

ip private enable

If you desire to set your own private ip addressing space, you must configure two commands:

Enable the private IP gateway:
ip private config <ip> mask <mask>
ip private enable

Configure the private IP network:
dhcp server disable
dhcp server config network private start <ip> end <ip>
dhcp server enable

For example:
ip private config 1.2.3.4 mask 255.255.255.0
ip private enable
dhcp server disable
dhcp server config network private start 1.2.3.101 end 1.2.3.125
dhcp server enable

NOTE: The DHCP server will not disable if any WallPlates already have an IP address. It is best to change the DHCP server config before the WallPlates link, or else you must disable the DSL ports and re-enable them after the configuration is complete.

To disable all DSL ports and remove DHCP address: *interface dsl disable port(1-25)*

Public IP address

If you wish to use 802.1x authentication, or if you wish to use ping to monitor the Wireless WallPlates, you must set the DHCP pool as a public pool. Note the following steps are required:

Disable the private IP gateway address: *ip private disable*

Configure the public IP network:
dhcp server disable
dhcp server config network public start <ip> end <ip>
dhcp server enable

For example:
ip private disable
ip config ip-address 10.1.1.2 mask 255.255.255.0 gate 10.1.1.1
dhcp server disable
dhcp server config network public start 10.1.1.101 end 10.1.1.125
dhcp server enable

NOTE: The public pool must be in the same subnet as the IP address of the T3 Switch.

Static IP address pool

Static leases can be added for the public IP address pool. To use a static lease, you must know the MAC address of the radio and the IP you wish to assign. To get a list of MAC addresses, first link the Wireless WallPlates via the standard DHCP server configuration. View the list using, ***"show dhcp server lease"***. The list of MAC addresses can be used to create the static lease table.

The MAC address of the radio is printed on the product serial label. Also, the MAC addresses will appear in the forwarding bridge. To view the forwarding bridge table, type ***"show bridge address"***

Disable the private IP gateway address: *ip private disable*

Configure the static lease entry:
dhcp server disable
dhcp server static-lease add <mac address> ip <ip>
dhcp server enable

Configuring a WLAN

Four steps are required to enable a WLAN and start broadcasting:

Step1: Create a profile to contain the SSID and per-SSID parameters

wifi wlan profile add <SSID>
ex: *wifi wlan profile add My_WLAN*

Step2: Bind the profile to a WLAN

wifi wlan config <wlan<1-25>-<1-16>> profile <SSID>
ex: *wifi wlan config wlan(1-25)-1 profile My_WLAN*

Step3: Enable the WLAN

wifi wlan enable <wlan<1-25>-<1-16>>
ex: *wifi wlan enable wlan(1-25)-1*

Step4: Enable the Radio

interface wireless enable <radio<1-25>>
ex: *interface wireless enable radio(1-25)*

Global Radio Commands

Use the following commands to Configure Global radio parameters:

Command	What it does
interface wireless enable/disable <radio<1-25>>	Enable the radio or disable the radio
Interface wireless config <radio<1-25>>	Channel: 1-11 Transmit power: 1-14, max (in dBm) Preamble: Auto, Long RTS-Threshold: 0-2347 Short Retry Limit: 1-255 Long Retry Limit: 1-255 Fragmentation: 256-2346 Mcast Rate Limit: 0-1000 Spectralink QoS: enable/disable Data Rate: 1, 2 … 54, Auto Max Client Association: 1-64 Beacon Period: 100-1000 (ms)
interface wireless wmm	Global WMM parameters for each radio
interface wireless mode	Set the mode to B, G, or B and G
interface wireless name	Assign a friendly name to the radio
interface wireless country	Select the operating country

Per-WLAN Commands

Use the following commands to configure per-WLAN parameters:

Command	What it does
wifi wlan profile add	Create a new WLAN by assigning an SSID as a profile name
wifi wlan profile config	Broadcast SSID: enable/disable Client Isolation: enable/disable Client inactivity timeout: 300-86400 (sec) DTIM Period: 1-255
Wifi wlan profile security	None: Dynamic-WEP: (uses 802.1x authentication) Static WEP: Key length, WEP key, Passphrase, Open or Shared WPA-personal: Preshared-key, version (WPA, WPA2, both) WPA-enterprise: version (WPA, WPA2, both), wpa2-pre-authentication

Monitor the WLANs and radios

Use the following commands to monitor the configuration and operational status of the WLANs:

Command	What it does
show wifi wlan	Config: displays administrative status Status: displays operational status Statistics: displays detailed WLAN statistics. Additional options are general, rate, size and qos
show wifi wlan profile	Config: displays administrative status Status: displays operational status
show interface wireless status	Displays operational status of the wireless radio
Show interface wireless statistics	Displays detailed statistics of the wireless radio
show wifi client statistics	Displays information about a connected client including MAC address, WLAN, and SSID

Expanded Statistics and Status

Most “show” commands display high level, important information for quick review. To see more detailed status or statistics, specify the actual radio or WLAN. For example;

displays high level status of all active radios *show interface wireless status*

displays detailed status of an individual radio *show interface wireless status radio1*

Access Control Lists (ACLs)

Configure layer 3 ACLs based on an administrator defined IP addresses and pre-defined services. The pre-defined services are HTTP, FTP, Telnet, SNMP.

Number of ACLs:	20
Each ACL index:	IP address
	pre-defined service
	combination of IP address and service

ACLs are processed from index 1 through index 20. If no matches are found, the access is granted.

Place the most restrictive access rules on the lower index number.

To enter ACLs from the CLI, use the following command:

ip access-list config <*1-20*(index)> <*deny*|*permit*(type)> [**ip-address** #.#.#.#] [**mask** #.#.#.#] [**service** *all*|*ftp*|*telnet*|*http*|*snmp*]

Ex: To block all HTTP access from any device, enter:

ip access-list config 1 deny http

Ex: To block all network access from all devices except Telnet from a specific subnet, enter:

ip access-list config 1 permit ip-address 64.174.72.129 mask 255.255.255.128 service telnet
ip access-list config 10 deny service all

Note: A 32-bit subnet mask will specify one single device with the specified IP address

RADIUS network authenticated login

RADIUS server configurations apply to administrative access accounts and client 802.1X authentication. RADIUS access-requests are supported, but RADIUS accounting messages are not. Up to five RADIUS servers can be added. The default RADIUS port 1812 is used and is not configurable.

Authenticating Administrative Access

RADIUS network authenticated logins allows the administrators to easily change all passwords by changing the password on the RADIUS server, simplifying management of a large network with multiple users.

To use RADIUS network authentication, you will need a properly configured RADIUS server (free RADIUS servers are available for Linux operating systems or fee-based server products are available on UNIX and Microsoft NOS).

RADIUS authenticated logins only support the "admin" user account privileges with the following exceptions:

- The RADIUS account cannot disable RADIUS login support
- The RADIUS account cannot change the built-in "Admin" password

Note: The "admin" account name is not reserved. You may create an "admin" account on the RADIUS server. If so, the T3 will first check the password against the local "admin" account password before trying the RADIUS server. Unless there is a special reason to do so, we recommend not using an "admin" account on the RADIUS server

Authenticating Clients using 802.1X

To use RADIUS authentication, the server must support 802.1X protocol and a supported EAP type. Supported EAP types are TLS, TTLS, and PEAPv0 (also known simply as PEAP)

Configure the RADIUS Server

To create a RADIUS server configuration from the CLI, use the following command:

radius server config <*1-5*(index)> <**ip-address** #.#.#.#> <**shared-secret** *string*> <**timeout** *1-10*> <**retries** *1-120*>

Options	Description
Index	5 RADIUS servers can be added. Authentication will be performed starting with the server in index 1
ip-address	IP address of the RADIUS server
shared-secret	This is the password used by the RADIUS server to authentication the Access-Request packets from the Tut OS
Timeout	Number of seconds to wait after sending an Access-Request packet before sending another request or trying another server. Practical timeout value is 5 seconds.
Retries	Number of retries before giving up and trying a different server. A practical entry for retries is 2 to 3.

WallPlate Installation

Basic Configuration

The following commands will enable a basic network configuration. The T3 system will ignore the text following the "#" comment character.

NOTE: Telnet is recommended due to the TCP flow control. Ranged commands can take several seconds to execute. If the console is used to paste a long string of commands, set a Line Delay of 500ms on your serial program so that the serial buffer does not overflow. If this happens, some commands may be lost or not executed.

Login using the serial console or telnet to the default IP address.

```
#BASIC IP AND SYSTEM CONFIGURATION
####################################
dhcp server enable
ip config ip <your IP address> mask <your mask> gateway <your gateway>
ip private enable
vlan enable
vlan mode local port remote tag
system reboot

#ENABLE AND CONFIGURE ONE WLAN
###################################
wifi wlan profile add <your SSID>
wifi wlan config wlan(1-25)-1 profile <your SSID>
wifi wlan enable wlan(1-25)-1

#ENABLE AND CONFIGURE DSL PORTS AND REMOTE ETHERNET PORTS
#########################################################################
interface dsl config port(1-25) max-down 10 max-up 10
interface remote enable port(1-25)-(1-2)

#ENABLE THE LINE POWER AND RADIO
###################################
interface wireless enable radio(1-25)
interface dsl po en port(1-25)

#REBOOT
########
system reboot
```

Tools Required:

Number 2 Philips head screwdriver

Note: if using a power drill, set the torque clutch to 5 in-lbs.

Components provided with the MC-802 WallPlate:

1 – MC-802 WallPlate
1 – RJ11 wall jack mounting adapter
1 – 100mm (4") RJ11 pigtail cable
2 – 6-32 thread forming Philips head screws, 0.375"

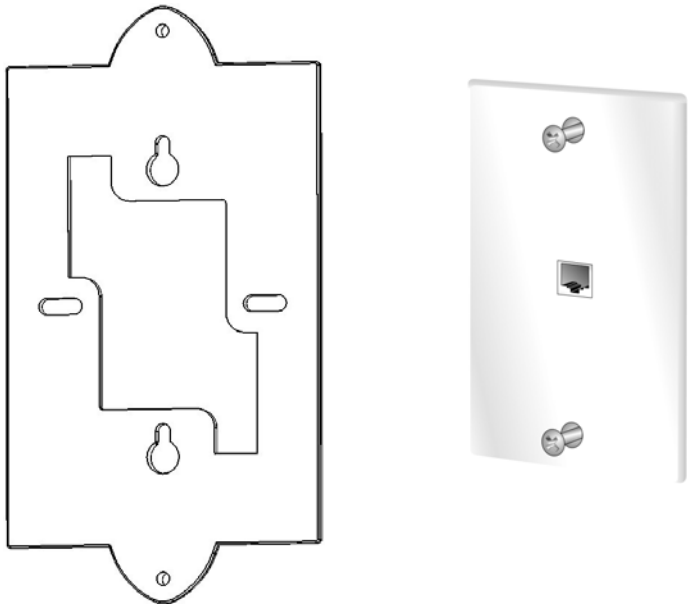
Components required to purchase:

Regulated 12V power supply. Use of the wrong power supply could result in damage to your WallPlate unit. Please order a small quantity of regulated 12V power supplies from Motorola to use during installation.

If you do not have the correct regulated 12V power supply – **STOP**. Order a regulated 12V power supply from your Motorola PBN sales representative.

Step 1

1. Loosen screws on wall plate approximately 6mm (1/4”)
2. Attach the bracket using the keyhole slots
3. Tighten screws until the bracket is firmly attached, do not over tighten

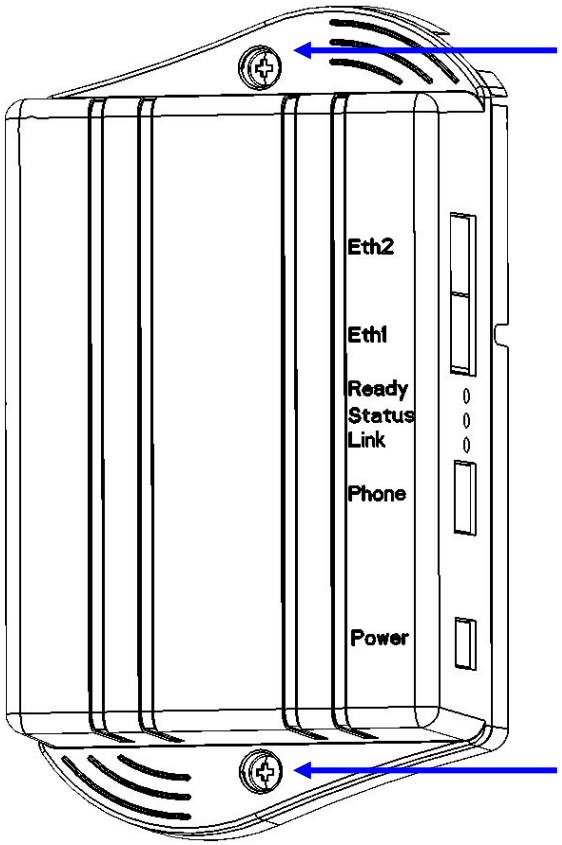


Step 2

Connect 50mm (2”) cable (supplied) between bottom mounted RJ11 port on the MC-802 and the existing RJ11 jack.

Step 3

Attach the MC-802 to the Mounting Adapter using the supplied 6/32 thread forming screws



6/32 thread forming screws

6/32 thread forming screws

Step 4

1. Connect the local AC power adapter to the WallPlate
2. Connect the analog phone to the RJ11 phone jack

Step 5

After WallPlate Link LED is solid, verify the device is connected using the command, “show int dsl status”. It is best to have a technician in the phone room directly connected to the T3 Switch to coordinate and enable Line Power.

Enable line power

Determine which port is being installed

From the CLI, enter this command:

show bridge address

The MAC address of the PC will appear along with the connected line.

Enable line power

From the CLI, enter this command:

*interface dsl power enable port**x*** (enable only the port being installing)

Finish the installation

Remove the 12V regulated power supply. If the correct port is enabled for line power, the WallPlate will reset and operate from in-line power.

802.1Q VLANs

Note: The system requires a reboot after the “vlan enable” command. If the system is not rebooted, the webUI will not display the VLAN configuration and the CLI will not execute VLAN commands.

VLAN Specification

VLAN modes:	IEEE 802.1Q standard compliant VLANs or Port-based VLANs on T3 Switch IEEE 802.1Q standard compliant VLANs on WallPlates
Max number of VLANs:	128 VLANs can be created on the T3 Switch and assigned to any port. 16 total VLANs can be assigned to interfaces on the Wireless WallPlate.
Valid VID range:	1 – 4094
Default PVID:	1
Default Egress:	transmit untagged
Default Ingress:	Accept all packets

VLAN terminology

The T3 Switch is a VLAN switch. The WallPlate is also a VLAN switch. Therefore, be certain that packets traversing the DSL links between the T3 Switch and the WallPlate are always TAGGED.

PVID	In the 802.1Q standard, each port is assigned a PVID. This is the default VLAN ID assigned to ***untagged packets*** received (ingress) on that port. The PVID is sometimes called the port Native VLAN. By default, all ports are assigned VLAN 1.
Tagged	T3 will optionally tag packets when transmitting (egress) on the port. Set the port as a tagged member of the VLAN by using the *vlan membership egress* command. On the T3 Switch, the tag ***mode*** (whether a packet transmits with a tag or not) of a packet is determined PER VLAN, not per port. This allows the T3 to support complex VLAN configurations not possible on other switches. On the WallPlate, the tag mode of a packet is determined PER PORT, similar to the Cisco IOS “trunk” mode.
Untagged	T3 will optionally transmit (egress) packets without an 802.1Q VLAN tag. Use Untagged packets on any port that is connected to a non-VLAN aware device. For example; if a PC is connected to the WallPlate ports, packets will be untagged. This is similar to the Cisco IOS “access” mode of a switchport.

Tag-based VLAN Mode	Tag based mode is fully 802.1Q VLAN compliant. You must explicitly configure the Egress and Ingress rules for each port and each VLAN. On the webUI, use the 802.1Q TAG-BASED VLAN menu to configure VLANs. The T3 Switch and WallPlate can operate independently. Be sure to configure all ports on the Switch and the WallPlates for proper operation.
Port-based VLAN Mode	Port based VLAN is also called Port Isolation or Port Privacy in other switches. When operating in port-based mode, the T3 Switch will ignore 802.1Q VLAN tags. Port isolation is based on a VLAN Map. On the webUI, use the PORT-BASED menu to see the VLAN Map and change the mapping. See below for more details. ***Note:*** The Switch operates in port-based or tag-based mode; whereas the WallPlates only operate in tag-based, or disabled. This allows for special case configurations where the WallPlates do all the 802.1Q VLAN tagging, while the Switch maintains port-to-port privacy.

VLAN commands

All VLAN configurations are also available from the webUI.

vlan config default	Restore VLAN configuration to default
vlan enable/disable	Enable or disable VLAN support. Requires a system reboot after issuing this command.
vlan add	Create or modify a VLAN and optionally assign a name.
vlan delete	Delete a VLAN Group. Remove all ports that are members of the group before deleting the group.
vlan membership add	Add or delete a VLAN from a port. Allows the VLAN to transmit on the port
vlan membership egress	Sets how a VLAN will egress; with a tag or without. By default, packets will transmit untagged unless specified using this command. Note this command does NOT apply to WallPlate ports
vlan membership delete	Deletes a port from a VLAN membership
vlan interface ingress	Ingress command: Assign the PVID for a port. This VLAN ID will be assigned to all packets received *untagged* on this port
vlan interface egress	Set the Egress mode on any CPE port. This command does not apply to T3 Switch ports
vlan interface igmp	Assign VLAN for IGMP packets
vlan interface mgmt	Assign VLAN for layer 2 security for all management traffic
vlan mode	Set the mode of operation on the Switch and the WallPlates. Options are IEEE 802.1Q tag-based, or Port-based. ***Note:*** WallPlates only support tag-based or disabled.
vlan port-group	CLI command to add ports to a Port-based VLAN.

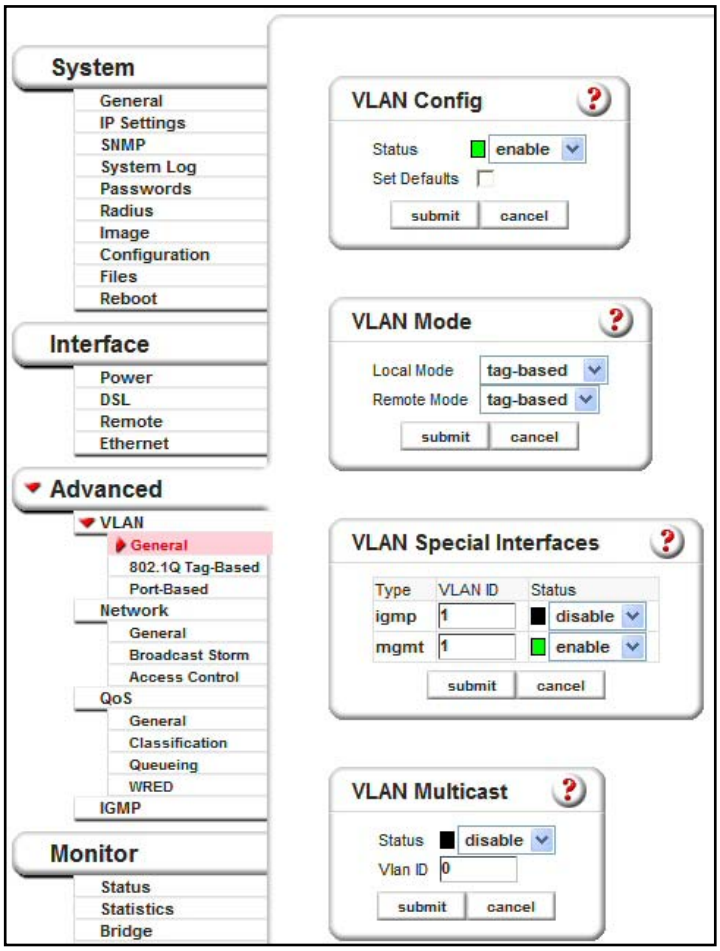
RADIUS network authenticated login	
show vlan membership	Displays the memberships in Rows and Columns
show vlan interface	Displays the PVID, Membership, and Mode in Rows and Columns

Web UI configuration

VLANs can be configured from the CLI, web UI or SNMP. The CLI advantage is support for scripting the entire configuration. The CLI disadvantage is the large number of commands required to execute the complete configuration.

The web UI is slower since it relies on Javascript running on your local PC, and the overhead associated with transmitting the configuration data. The graphical display is easy to follow and should be used to get familiar with the system.

Vlan General webUI



VLAN Config
Enable VLAN support. Requires system reboot.

VLAN Mode
Local Mode refers to the T3 Switch. Port-based or Tag-based is supported. Remote Mode refers to the WallPlate. Tag-based or disabled is supported.

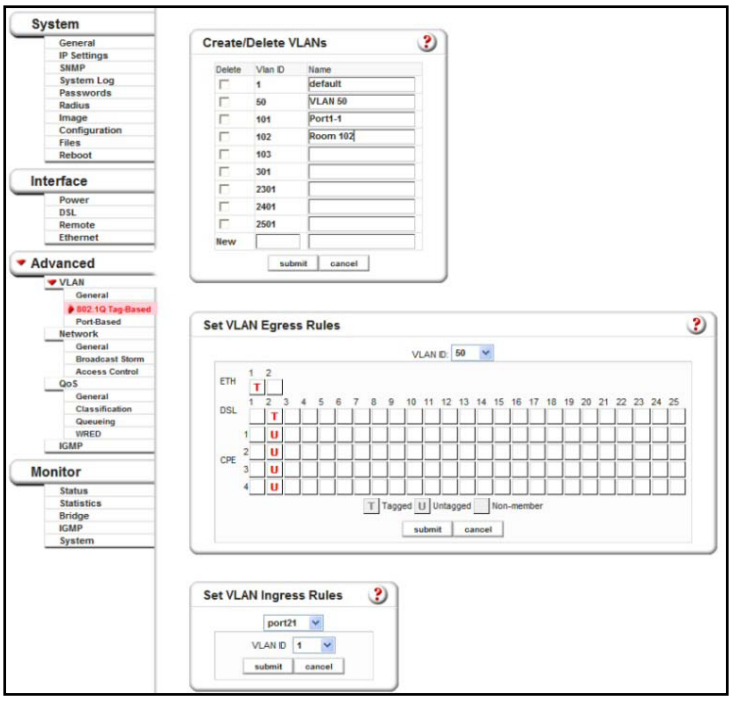
VLAN Special Interfaces
If video is delivered on a defined “video VLAN”, be sure to assign IGMP to the VLAN used for video. When IGMP Proxy is enabled, T3 will proxy IGMP packets with the VLAN ID of the group in this configuration.

Management packets can be tagged with a specific VLAN ID for layer 2 security. Enable management VLANs and assign a VLAN ID.

The VLAN must first be created using the 802.1Q Tag Based menu.

VLAN Multicast
Enable multicast support and assign the VLAN where multicast packets will be sent. This VLAN should be the same as the IGMP VLAN ID for proper delivery of video.

Tag-based VLAN webUI



Create/Delete VLANs

Use this menu to create new VLANs and assign a name to the VLAN. Note that you cannot delete VLAN 1, however VLAN 1 can be removed from all interfaces.

Set VLAN Egress Rules

Set the VLAN membership rules.
Click 3 times in the box to select (**U**)ntagged, (**T**)agged or not a member. In this example, Eth1 is a (**T**)agged member of VLAN 50.

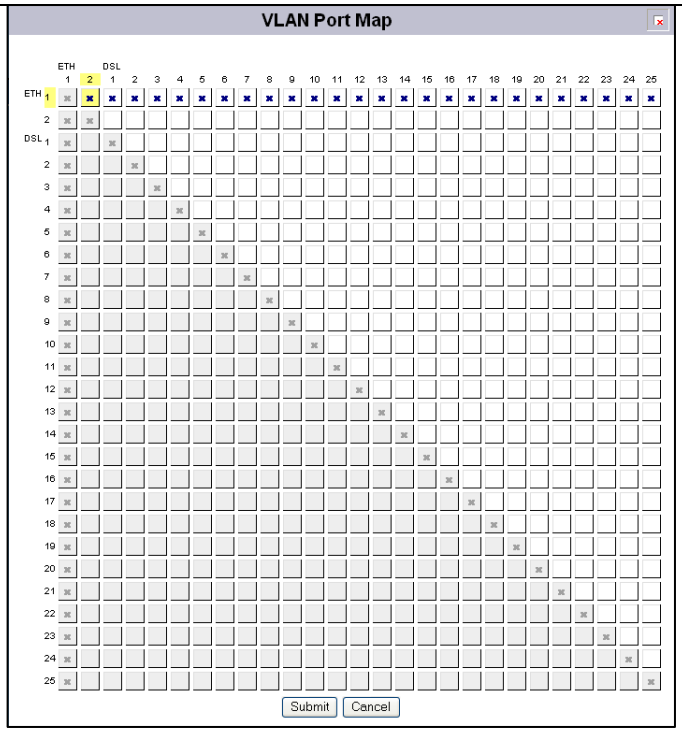
DSL ports will always be a (**T**)agged member of any VLANs on the connected WallPlate

In this example, Port 1 of the first WallPlate is an (**U**)ntagged member of VLAN 50.

Set VLAN Ingress Rules

Set the PVID for each port. This is also known as the native VLAN for the port. All packets received on these ports (as from a PC connected to the port) are assigned the PVID of the port

Port-based VLAN webUI



When the local mode is set to Port-based (The T3 Switch is the local mode), use the Port-based menu to create a Port Map.

By default, Eth1 and Eth2 can communicate with each other. All DSL ports can communicate with Eth1 and Eth2, but **NOT** with each other.

The example at right shows an effective way to configure port privacy on all DSL ports, and configure Eth2 as a cascade port. This example can be replicated on all Switches in a cascade for simple, effective port privacy.

Note:

- Eth1 can communicate with Eth2
- Eth1 can communicate with all DSL ports
- Eth2 cannot communicate with all DSL ports
- DSL ports cannot communicate with each other

Port-based VLAN webUI, continued

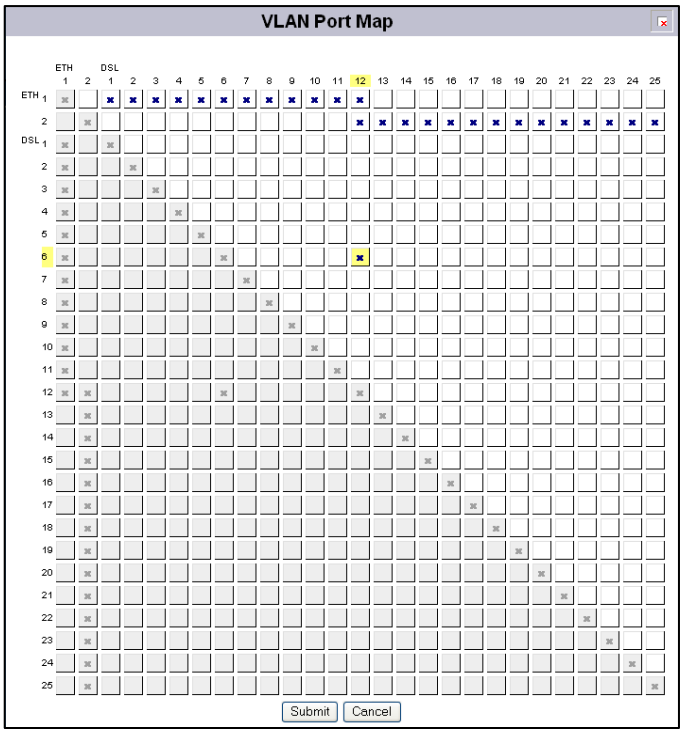
In the example at right, Note:

- Eth1 and Eth2 cannot communicate together
- Eth1 can communicate with DSL ports 1 – 12
- Eth2 can communicate with DSL ports 12 – 25
- Port 12 can communicate with both Eth1 and Eth2
- Ports 6 and 12 can also communicate together

Note that DSL ports can only talk to the upstream Eth1 or Eth2. The only exception is DSL ports 6 and 12.

Port-based mode on the T3 Switch can be mixed with Tag-based mode on the WallPlate for an effective method to configure VLANs for advanced services.

Note VLAN Tutorial One for an example of mixing Port-based and Tag-based VLANs.



Quality of Service (QoS)

Standards	IEEE 802.1P, WRED, WFQ, IP TOS based on RFC1275
Number of queues	4 queues per port
Packet classifiers	Static classifier: All packets received on a port are assigned to a single queue Dynamic classifier: Packets are assigned to a queue based on their IP TOS or 802.1P
WFQ queue mode	Administrator selectable queue weight. Queue weights are calculated as a percentage of the cumulative weights. Using WFQ, any queue can burst up to the maximum bitrate of the line. This can occur if no packets in a higher priority queue are waiting to transmit. If you wish to apply strict rules and limit a low priority queue to a fixed amount, use the "egress shaping" command.
Priority queue mode	Strict priority over all lower queues. Note that Priority queuing can be mixed with other queuing methods to provide a low latency, low jitter service for sensitive services such as VoIP. For example, if the critical queue were assigned a Priority mode, then those packets would transmit on the port before other packets in the buffers.
Shaping queue mode	Apply traffic shaping rules to individual queues. Each queue is assigned a fixed amount of bitrate. The cumulative bitrate of all the queues should not exceed the total line rate of the port.

QoS commands and concepts

network qos [enable | disable]

Enable qos support. To disable qos, use *network qos disable*

network qos interface priority <interface-id> mode <mode> [level <level>]

Sets the packet classifier mode for the port receiving packets.

Where;

Mode is *dynamic* or *static*. Dynamic classifier will read the IP TOS or 802.1P precedence bit of the incoming packet. Static classifier assigns all packets received on the port to one of the four queues

Level is the default queue for packets received on the port. When the mode is dynamic, then level is assigned to packets that do not match the classifier. When the mode is set to static, then level applies to all packets received on the port.

The four queues are *critical, high, medium,* and *low*.

network qos classification <method>

where **method** is either *802.1p* or *tos*

Once a port has been set to use dynamic or static mode; specify whether T3 will use IP TOS or 802.1P precedence bit for dynamic packet classification.

network qos interface queue <interface-id> mode <mode>

Deprecated commands to set the queuing mechanism on a port. This command is superseded by *network qos interface egress* which has more configuration options.

When using this command, note that WFQ has a fixed percentage for each queue:

Critical: strict priority over all other queues
High: 70% of available bitrate
Medium: 20% of available bitrate
Low: 10% of available bitrate

In priority mode, strict priority applies to all queues where a higher queue always transmits before a lower queue.

Note that when using wfq mode, a low priority queue will use all the available bandwidth if a higher priority queue is not in the transmission buffer.

network qos interface egress priority <interface-id> queue <queue>

Any queue assigned as a Priority queue will transmit using strict priority. A higher level queue will always transmit before a lower level queue. Use priority mode for latency and jitter sensitive applications.

network qos interface egress shaping <interface-id> queue <queue> peak <peak rate> average <avg rate> burst <burst size>

Set a fixed traffic shaping parameter for each queue. Note that a queue will never exceed the peak rate parameter regardless of other services on the port.

Where;

Queue: the queue where you wish to shape traffic. Valid options are critical, high, medium, or low
Peak: the maximum rate for the queue, in Mbits/second
Average: the average rate for the queue, in Mbits/second
Burst: the maximum data burst allowed at the peak rate

network qos interface egress wfq <interface-id> queue <queue> weight <0-200>

Configure the behavior of the WFQ scheduling method. Bitrates are determined as a percentage of the total queue weights.

In order to determine the percentage of bandwidth that will be allocated for a particular queue, divide the queue weight by the sum of all the queues “weight”.

For example; assume the ***High queue*** weight is 100 and the ***Medium queue*** weight is 50. 100 + 50 = 150. So, the High queue will receive 66% of the bandwidth (100/150=0.667) and the Medium queue will receive 33% of the bandwidth (50/150=0.33).

network qos multicast config queue-allocation <allocation>

Multicast packets are allocated a separate set of transmission buffers. Set the multicast queue to be the same queue where the multicast packets will be transmitted. For example, if using video packets with an IP TOS bit, assign the packets to the high queue based on the IP TOS bit, and assign the multicast queue to be also use high. T3 has no way to automatically determine where the multicast packets will be transmitted.

network qos wred enable | disable

Enable or disable WRED support. WRED adds further protection for data integrity in a contention based Ethernet network by randomly discarding TCP packets according to administrator settable parameters for thresholds.

network qos wred config min-discard <min-discard> max-discard <max-discard>

Set the rate at which Ethernet frames will be discarded once the rate exceeds the thresholds. Note that two discard rates are supported. Min-discard is the rate that frames are discarded when they reach the minimum configured threshold. Max-discard is the rate that frames are discarded when they reach the maximum configured threshold. Often, the max-discard rate will be set to 100.

network qos interface wred <eth<1-2>|port<1-25>(interface-id)> <queue low|medium|high|critical> <min-threshold 1-100> <max-threshold 1-100>

Set the minimum and maximum buffer threshold for each queue, on each port. Once either threshold is crossed, frames are discarded at the discard rates specified by the *network qos wred config* command.

Dynamic packet classification

In dynamic mode, packets are classified by the 802.1P Ethernet precedence bit or IP TOS (precedence bits) in the Diffserv byte. This definition is taken from the latest RFC 2475. Note that the IP TOS bits are defined as the three most significant bits of the DiffServ byte.

Ethernet frames are mapped to transmission queues based on the following chart:

802.1P bit	IP TOS	Queue
0	0	Low
1	1	Low
2	2	Medium
3	3	Medium
4	4	High
5	5	High
6	6	Critical
7	7	Critical

QoS Example

An easy way to demonstrate QoS is to use the traffic shaping queue scheduler. To further simplify the example, dynamic packet classifier is not used.

Packet Classification:

Static. All packets on Eth1 will be classified high. All packets on Eth2 will be classified low.

Packet transmission:

Shaping. All four queues will be configured with unique bitrates.

Connections:

A SmartBits network tester can be used; however the same QoS results can be easily demonstrated using iperf and four PCs. In either case, one flow will be connected from Eth1 of the T3 Switch to Port1-1 of the first WallPlate. The other flow will be connected to Eth2 of the T3 Switch and Port1-2 of the first WallPlate.

Commands:

network qos enable
system reboot

network qos interface priority eth1 mode static level high
network qos interface priority eth2 mode static level medium

network qos interface egress shaping port1 queue critical peak 30 average 30 burst 100
network qos interface egress shaping port1 queue high peak 20 average 20 burst 100
network qos interface egress shaping port1 queue med peak 10 average 10 burst 100
network qos interface egress shaping port1 queue low peak 5 average 5 burst 1

Note that the PCs connected to Eth1/Port1-1 will receive 20Mbps bitrate; whereas the other PCs will receive 10Mbps bitrate. While the test is running, change the static level command and watch the behavior change.

network qos interface priority eth1 mode static level low

Line Status

Operators can view extensive details about DSL line characteristics from the CLI, Port Monitor web page, or SNMP.

To view line characteristics using the webUI, click on DSL Monitor, then click the + sign to expand the port you wish to view.

Using the Port Monitor web page, the operator can quickly scan the status of all ports in the system. A color coded grid indicates the important status of each port e.g. GREEN indicates the Ethernet port is connected, whereas GREY indicates the port is enabled, but disconnected.

Per line details visible:

Status	Options are self-explanatory: disabled, enabled, linking, link lost, linked.
Quality	Link quality is a measurement of bit errors per second. Options are: Good, Fair, Bad. T3 includes Forward Error Correction in the VDSL frames. Bit errors that are not corrected are counted and reported as a Line Quality measurement. Bit errors of 0 – 0.51 per second = Good Bit errors of 0.51 - 1 per second = Fair Bit errors of greater than 1 per second = Bad
Portx	Where “x” is the number of a remote Ethernet port on the WallPlate. Shows the status of the remote Ethernet port. Options are: connected, disconnected, disabled.
Downstream	Displays the line bitrate in the downstream direction in Mbits/second.
Upstream	Displays the line bitrate in the upstream direction in Mbits/second.
SNR DSx **SNR USx**	Where “x” is 1 or 2. T3 uses a 4-band QAM modulation. Three of the 4 bands are used by T3 to maximize downstream line bitrate. DS1 and DS2 refer to the two downstream bands; whereas US1 refers to the single upstream band. If a band shows 0 SNR, the band is not being used by that line. During normal operation, it will be common to see 0 SNR on DS2. US2 will always show 0, this is normal. SNR can be used to diagnose line issues, but must be considered in concert with other parameters. Values are in dB.
Margin DSx **Margin USx**	Each band requires SNR to be reserved as for margin. Typical values of SNR margin is between 6 and 9. If margin is lower than 6, the line may have low quality and may retrain at any time. If margin is greater than 9, the line is capable of a higher bitrate. Any band that is not being used will show a margin of 0. Values are in dB.
Distance (m)	Distance value shows estimated line length in meters, based on the level of the attenuated signal. Distance is accurate within 10% over 150m. Measurements below 150m are displayed at <150.

Line Current

This value indicated the total power consumed by the port; including power loss in the wire, in the WallPlate, and efficiency.

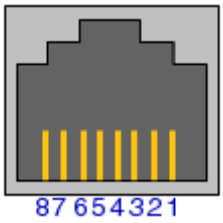
Maximum power for any single line: 9 watts
Maximum line power for a complete system: 200 watts

To determine the power for a single line use the following chart:

Line Current Value	Watts	Reference
255	2.58	Idle, no load or wire attached
197	4.87	
195	4.91	
190	5.02	
185	5.13	
180	5.31	
175	5.38	
170	5.49	
165	5.60	
162	5.71	
160	5.82	
155	5.93	
150	6.11	
145	6.25	
140	6.40	
135	6.58	
130	6.80	
125	7.02	
120	7.24	
115	7.45	
113	7.53	
112	7.64	
110	7.71	
105	7.93	
100	8.18	
95	8.47	
90	8.76	
85	9.13	Maximum Power supported for the line
80	9.45	
75	9.85	
70	10.29	
65	10.76	
60	11.27	
55	11.78	
50	12.36	*Out of spec*
45	13.05	
40	13.64	
35	14.40	
30	15.53	
25	16.33	
20	17.49	

Appendix A: Pin-out Assignments

Fast Ethernet WallPlate ports



1	TX+
2	TX-
3	RX+
4	Unused
5	Unused
6	RX-
7	Unused
8	Unused

Appendix B: Hardware Specifications

T3 PowerBroadband

Line code modulation	3-band, QAM modulation Automatic power backoff, independent line-rate adaptation
Interfaces	2 x RJ45, 10/100/1000Mbps auto-sensing – 328ft (100m) 2 x RJ21, female telco connector 1 x DB9, female console port
Operating Voltage	100 – 240VAC, 50/60Hz
Power Consumption	300 Watts
Dimensions	17.25” x 14.25” x 1.75” (43.8cm x 36.1cm x 4.4cm)
Weight	11.5lbs (5.2Kg)
Environmental	Operating Temperature: 0 – 50 degrees Celsius, fan cooled
Relative Humidity	5% to 90% NC
Compliance	FCC Part 15A, CE, TUV EN60950
Telephone splitter	Integrated analogue POTS splitter
Management	In Band Management Telnet, Web UI, SNMP v2 standard and enterprise MIB Out of Band Management Console
Front Panel LEDs	1 x unit power status 25 x line link status 10/100/1000 link status
Mounting Options	Rack mount ears provided

m2 WallPlate

Interfaces	2 x RJ45, 10/100Mbps auto-sensing – 328ft (100m) 1 x RJ11, line-in port 1 x RJ11, filtered phone port
Operating Voltage	Local power supply (not provided): 12VDC, regulated supply
Power Consumption	2 watts
Dimensions	4.75” x 3.5” x 1.25” (120mm x 88mm x 32mm)
Weight	0.5lbs (0.2Kg)
Environmental	Operating Temperature: 0 – 50 degrees Celsius
Relative Humidity	5% to 90% NC
Compliance	FCC Part 15A CE, TUV EN60950, ETSI EN 301 489-1, 17

Telephone splitter	Integrated analog POTS splitter
Management	In Band Management Telnet, Web UI, SNMP v2 standard and enterprise MIB
Front Panel LEDs	1 x unit power/link status 10/100 link status, activity
Mounting Options	Mounting bracket provided

MC-802 Wireless WallPlate

Interfaces	2 x RJ45, 10/100/Mbps auto-sensing – 328ft (100m) 1 x RJ11, line-in port 1 x RJ11, filtered phone port
Input Voltage	Local power supply, 12VDC (not shipped)
Power Consumption	6 watts
Dimensions	3.75” x 6.75” x 1.75”
Weight	11 oz
Environmental	Operating Temperature: 0 – 40 degrees Celsius
Relative Humidity	5% to 90% NC
Compliance	FCC Part 15A, CISPR 22 FCC Part 15C 15.247 ETSI ETS 300 328 2.4Ghz EN 55022 : 1994/A1 : 1995/A2 : Class A EN 55024 : 1998 : Class A CE, TUV EN60950 RoHS 2002/95/EC ANZ C-Tick
Telephone splitter	Integrated analog POTS splitter
Management	In Band Management Telnet, Web UI, SNMP v2 standard and enterprise MIB
Front Panel LEDs	1 x Ready, power status 1 x Status, software booted, errors 1 x Link, xDSL link training 10/100 link status, activity
Mounting Options	RJ11 wall plate mounting adapter provided